IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

ALEXANDRIA DIVISION

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH NAME USER IDENTIFICATION NUMBER 1142201852792934541 STORED AT PREMISES CONTROLLED BY DISCORD, INC.	Case No. 1:24-SW-592 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Olivia Temrowski, a Special Agent of the Federal Bureau of Investigation, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this Affidavit in support of an application for a warrant to search for information associated with the following account: User identification number ("UID") 1142201852792934541, believed to have been utilized by MICHAEL DAVID SEEDS ("SUBJECT"), which is stored at premises controlled by Discord, Inc. ("DISCORD"), an electronic communications and remote computer services provider, which accepts service of legal process at 444 De Haro Street, Suite 200, San Francisco, CA, 94107.

2. I describe the information to be searched in the following paragraphs and in Attachment A. I make this Affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require DISCORD to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment

B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

3. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been so since 2020. I am thus a "federal law enforcement officer" as defined by Fed. R. Crim. P. 41(a)(2)(C) and am authorized by law or by a Government agency to engage in or supervise the prevention, detection, investigation, or prosecution of violations of federal criminal laws. As part of my duties as a Special Agent, I am currently assigned to the FBI Washington Field Office's Child Exploitation and Human Trafficking Task Force ("CEHHTF"). In my current assignment, I investigate violations of federal law, including the online sexual exploitation of children. This includes violations pertaining to the illegal possession, receipt, distribution, transmission, advertisement, and production of material depicting the sexual exploitation of minors. I hold a Master's Degree in Social Work from the University of Michigan and am a Licensed Master of Social Work. I am a graduate of the FBI Academy in Quantico, Virginia where I received extensive training in federal law and various investigative methods. I have written, executed, and/or participated in the execution of numerous search warrants, to include search warrants of social networking platforms. I have gained experience in the investigations of child pornography and child exploitation through training and discussions with other law enforcement officers.

4. Based upon the information provided in this Affidavit, I respectfully submit that there is probable cause to believe that evidence of violations of Title 18, United States Code §§ 2252 (Activities Relating to Material Involving the Sexual Exploitation of Children), 2252A (Activities Relating to Material Constituting or Containing Child Pornography), and 2251 (Sexual Exploitation of Children), (hereinafter referred to as "SUBJECT OFFENSES"), is currently located within the data associated with the **TARGET ACCOUNT**, as more fully described in

Attachment B. There is also probable cause to search the information described in Attachment A for instrumentalities, contraband, or fruits of these crimes, further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested Warrant because it is a "court of competent jurisdiction" as defined by 18 U.S.C. §§, 2703(a), 2703(b)(1)(A), 2703(c)(1)(A), and 2711. Specifically, this Court is "a district court of the United States . . . [that] has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

BACKGROUND CONCERNING DISCORD AND ELECTRONIC COMMUNICATIONS SERVICES

6. Based on DISCORD's Privacy Policy, last updated March 15, 2024 and effective April 15, 2024, and available online at discord.com/privacy, I know the following about the collection of preservation of data at DISCORD:

a. DISCORD collects information from users when they voluntarily provide information, such as when they register for access to the DISCORD application and related Internet services (the "Services"). Information DISCORD collects may include, but is not limited to, username, email address, and any messages, images, transient VOIP data (to enable communication delivery only), or other content users send via the chat feature.

b. When users interact with DISCORD by using its Services, DISCORD receives and stores certain information such as an IP address, device ID, and the user's Services activities. DISCORD may store this information in databases owned and maintained by affiliates, agents or service providers. The Services may use this information and pool it with other information to track, for example, the

total number of visitors to DISCORD's website, the number of messages users have sent, and the domain names of visitors' Internet service providers.

c. DISCORD may conduct research on its customer demographics, interests, and behavior based on the information collected. This research may be compiled and analyzed on an aggregate basis, and DISCORD may share this aggregate data with its affiliates, agents, and business partners. DISCORD may also disclose aggregated user statistics to describe its Services to current and prospective business partners, and to third parties for other lawful purposes.

d. Users may give DISCORD permission to collect their information in other services. For example, a user may connect a social networking service such as Facebook or Twitter to their DISCORD account. When a user does this, it allows DISCORD to obtain information from those accounts (for example, a user's friends or contacts).

e. DISCORD uses cookies and similar technologies to keep track of users' local computer settings such as notification settings and which account users have logged into the Services. Cookies are pieces of data that sites and services can set on a user's browser or device that can be read on future visits. DISCORD may expand its use of cookies to save additional data as new features are added to the Services it provides. In addition, DISCORD uses technologies such as web beacons and single-pixel gifs to record log data such as open rates for emails sent by the system.

f. DISCORD may use third party website analytic tools such as Google Analytics on its website that use cookies to collect certain information concerning use of

its Services. However, users can disable cookies by changing their browser settings.

g. A user may see a DISCORD Service advertised in other applications or websites. After clicking on one of these advertisements and installing a DISCORD Service, the user will become a user of the Service. Advertising platforms, which include Twitter and Facebook (and whose software development kits are integrated within DISCORD's Service), may collect information for optimizing advertising campaigns outside of the Service.

7. In my training and experience, I have learned that providers of e-mail and/or social media services offer a variety of online services to the public. Providers, like DISCORD, allow subscribers to obtain accounts like the TARGET ACCOUNT. Subscribers obtain an account by registering with the provider. During the registration process, providers generally ask their subscribers to provide certain personal identifying information when registering for an e-mail or social media account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). Some providers also maintain a record of changes that are made to the information provided in subscriber records, such as to any other e-mail addresses or phone numbers supplied in subscriber records. In my training and experience, such information may constitute fruits, evidence, and instrumentalities of violations of the TARGET OFFENSES because the information can be used to identify the user(s) of an account.

8. Therefore, DISCORD's computers are likely to contain stored electronic communications and information concerning subscribers and their use of DISCORD's services,

such as account access information, e-mail or message transaction information, and account application information. In my training and experience, such information may constitute fruits, evidence, and instrumentalities of violations of the TARGET OFFENSES because the information can be used to identify the user(s) of an account.

9. A subscriber of a service provider, such as DISCORD, can also store with the service provider files in addition to e-mails or other messages, such as address books, contact or buddy lists, calendar data, pictures or videos (other than ones attached to e-mails), notes, and other files, on servers maintained and/or owned by the service provider. In my training and experience, evidence of who was using an account may be found in such information.

10. In my training and experience, e-mail and social media providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of login (session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, e-mail and social media providers often have records of the IP address used to register the account and the IP addresses associated with logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the target accounts.

11. In my training and experience, e-mail and social media account users will sometimes communicate directly with the service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Providers of e-mails and social media services typically retain records about such communications, including records

of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute fruits, evidence, and instrumentalities of violations of the TARGET OFFENSES because the information can be used to identify the user(s) of an account.

12. I know from my training and experience that the complete contents of an account may be important to establishing the actual user who has dominion and control of that account at a given time. Accounts may be registered in false names or screen names from anywhere in the world with little to no verification by the service provider. They may also be used by multiple people. Given the ease with which accounts may be created under aliases, and the rarity with which law enforcement has eyewitness testimony about a defendant's use of an account, investigators often have to rely on circumstantial evidence to show that an individual was the actual user of a particular account. Only by piecing together information contained in the contents of an account may an investigator establish who the actual user of an account was. Often those pieces of information will come from a time period before the account was used in the criminal activity. Limiting the scope of the search would, in some instances, prevent the government from identifying the true user of the account and, in other instances, may not provide a defendant with enough information to identify other users of the account. Therefore, the contents of a given account, including the e-mail addresses or account identifiers and messages sent to that account, often provide important evidence regarding the actual user's dominion and control of that account. For the purpose of searching for content demonstrating the actual user(s) of the TARGET ACCOUNT, I am requesting a warrant requiring DISCORD to turn over all information associated with the TARGET ACCOUNT with the date restriction included in Attachment B for review by the search team.

13. I also know based on my training and experience that criminals discussing their criminal activity may use slang, short forms (abbreviated words or phrases) or codewords (which require entire strings or series of conversations to determine their true meaning) when discussing their crimes. They can also discuss aspects of the crime without specifically mentioning the crime involved. In the electronic world, it is even possible to use pictures, images and emoticons—images or computer-key configurations used to express a concept or idea, such as a happy face inserted into the content of a message or the use of a colon and parenthesis :) to convey a smile or agreement—to discuss matters. "Keyword searches" would not account for any of these possibilities, so actual review of the contents of an account by law enforcement personnel with information regarding the identified criminal activity, subject to the search procedures set forth in Attachment B, is necessary to find all relevant evidence within the account.

14. In my training and experience, providers also keep a record of search queries run by the user of the account, whether searches within the services of the provider for persons, content, or other accounts (such as if a user is trying to find the account of an acquaintance), or broader Internet searches. In some instances, providers may also keep records of which websites or contents were "clicked on" as a result of these searches. This information is helpful both in the context of the case to show the topics about which the user was trying to obtain more information or conduct research, and is relevant for "user attribution" evidence, analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

15. I know based on my training and experience that providers of e-mail or social media services generally have access to and store the web or Internet browsing history of the user while he or she is logged into an account. That history can include names and specific websites or URLs/URIs (Uniform Resource Locators or Indicators) of the sites that have been visited.

16. I know based on my training and experience that providers of e-mail or social media services will often keep track of what is referred to as user agent string, which contains information about the type of computer, operating system, and web browser used to access the service. User agent string can include: web requests or HTTP requests (hypertext transfer protocol is the protocol by which many web pages are transmitted between servers and clients or users); logs containing information such as the requestor's IP address, identity and user identification number ("UID"), date and timestamp, request URL or URI (website address), HTTP protocol version, referrer, and similar information; login tracker logs; account management logs; and any other e-mail or social media accounts accessed by or analytics related to the target accounts. These can be used to determine the types of devices used while accessing the target accounts, as well as data related to the user's activity while accessing the target accounts.

17. Users of accounts are often required to include an e-mail account as well as a phone number in subscriber records. The e-mail account may be an e-mail account hosted at the same provider, or an account at a different provider. The e-mail account is referred to by several names, such as a secondary e-mail account, a recovery e-mail account, or an alternative e-mail account or communication channel. That e-mail account is often used when the identity of the user of the primary account (the target account) needs to be verified, for example if a password is forgotten, so that the provider can confirm that the person trying to access the account is the authorized user of the account. Similarly, the telephone number used in subscriber records is often used to send a passcode via text (or "SMS") that must be presented when trying to gain access to an account, either in a similar scenario where a user forgot his or her password, or when users implement what is referred to as "two-factor authentication" (where the password is one factor, and the passcode sent via text message to a mobile device is a second). In either scenario, the user of a primary e-

mail account (target account) and a secondary e-mail account or phone number listed in subscriber records are very often the same person, or at least are close and trusted and/or working in concert. That is because access to either the secondary e-mail account or to the phone number listed in subscriber records can allow access to the primary account.

18. Providers also frequently obtain information about the types of devices that are used to access accounts like the TARGET ACCOUNT. Those devices can be laptop or desktop computers, cellular phones, tablet computers, or other devices. Individual computers or devices are identified by a number of different means, some of which are assigned to a particular device by a manufacturer and connected to the "hardware" or the physical device, some are assigned by a cellular telephone carrier to a particular account using cellular data or voice services, and some are actually assigned by the provider to keep track of the devices using its services. Those device identifiers include Android IDs, Advertising IDs, unique application numbers, hardware models, operating system versions, unique device identifiers, Global Unique Identifiers or "GUIDs," serial numbers, mobile network information, phone numbers, device serial numbers, Media Access Control ("MAC") addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI"). Apple, one of the primary suppliers of mobile devices used to access accounts like the TARGET ACCOUNT, had previously used an identifier that was unique to the hardware of its devices, such that details of a device's activity obtained from a particular application or "app" could be used to target advertisements for the user of that device. Apple replaced that hardware-based identifier with the Apple advertiser ID or IDFA that is still

unique to a device, but which can be wiped and re-generated by a user if a user chooses to do so. Most users, however, do not know that the IDFA exists, and therefore are unaware that their device's activity can be correlated across different apps or services.

19. These device identifiers can then be used (a) to identify accounts accessed at other providers by that same device, and (b) to determine whether any physical devices found during the investigation were the ones used to access each target account. The requested warrant therefore asks for the device identifiers, as well as the identity of any other account accessed by a device with the same identifier.

20. Providers of e-mail and social media often maintain, have access to, and store information related to the location of the users of accounts they service. That information may be obtained by the provider in several ways. For example, a user may access the provider's services by running an application on the user's phone or mobile device, which application has access to the location information residing on the phone or mobile device, such as Global Positioning System (GPS) information. It may also be accessible through "check-in" features that some providers offer that allow users to transmit or display their location to their "friends" or "acquaintances" via the provider.

21. The subscriber will also generally need to use a password that will allow the user to gain access to the account. Many providers do not store the password directly, rather they use an algorithm (often referred to as a "hashing" algorithm) that is performed on the password and generates a new random of string of numbers and characters, which is what the provider may store. When a user enters his or her password, the hashing algorithm is performed on the password before it is presented to the provider, and the provider will verify the hash value for the password (rather than the password itself) to authorize access to the account. As an added security feature, some

providers insert additional text before or after the password, which is referred to as "salting" the password. The hashing algorithm is then performed on the combined password and salt, which is the hash value that will be recognized by the provider. Alternatively, or in addition to passwords, users may be required to select or propose a security question, and then provide an answer, which can be used to substitute for a password or to retrieve or reset a user's password.

22. This Application seeks a warrant to search all responsive records and information under the control of the service provider, which is subject to the jurisdiction of this Court, regardless of where the provider has chosen to store such information.

23. As set forth in Attachment B, I am requesting a warrant that permits the search team to keep the original production from DISCORD, under seal, until the investigation is completed and, if a case is brought, that case is completed through disposition, trial, appeal, or collateral proceeding.

24. I make that request because I believe it might be impossible for a provider to authenticate information taken from the target accounts as its business record without the original production to examine. Even if the provider kept an original copy at the time of production (against which it could compare against the results of the search at the time of trial), the government cannot compel the provider to keep a copy for the entire pendency of the investigation and/or case. If the original production is destroyed, it may be impossible for the provider to examine a document found by the search team and confirm that it was a business record of the provider taken from the target accounts.

25. I also know from my training and experience that many accounts are purged as part of the ordinary course of business by providers. For example, if an account is not accessed within a specified time period, it—and its contents—may be deleted. As a consequence, there is a risk

that the only record of the contents of an account might be the production that a provider makes to the government, for example, if a defendant is incarcerated and does not access his or her account. Preserving evidence, therefore, would ensure that the government can satisfy its *Brady* obligations and give the defendant access to evidence that might be used in his or her defense.

BACKGROUND CONCERNING SUBJECT OFFENSES

26. Title 18 U.S.C. § 2251(a) prohibits any person to employ, use, persuade, induce, entice, or coerce any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed.

27. Title 18 U.S.C. § 2252(a)(2) prohibits any person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any visual depiction using any means or facility of interstate or foreign commerce, or that has been mailed or shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproducing any visual depiction for distribution using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce or through the mails, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

28. Title 18 U.S.C. § 2252(a)(4)(B) prohibits any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

29. The term "minor," as defined in 18 U.S.C. § 2256(1), means any person under the age of 18 years.

30. The term "sexually explicit conduct," as defined in 18 U.S.C. § 2256(2)(A)(i)–(v), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

31. The term "visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data that is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

32. The term "child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor

engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

33. The term "child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors in sexually explicit poses or positions.

34. The term "computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones and devices. *See* 18 U.S.C. § 1030(e)(1).

35. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

CHARACTERISTICS OF INDIVIDUALS WITH A SEXUAL INTEREST IN CHILDREN OR VISUAL DEPICTIONS OF CHILDREN

36. Based upon my training and experience, as well as upon information provided to me by other law enforcement officers, there are certain characteristics common to individuals who

receive, possess and/or access with intent to view child pornography, which may be exhibited in varying combinations:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children, from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses (such as in person, in photographs, or other visual media), or from literature describing such activity. Due to the accessibility and availability of child pornography on the Internet, in my recent experience, instead of maintaining collections, some offenders engage in a pattern of viewing or downloading child pornography online and then deleting the material.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. They may also use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections can be maintained for several years to enable the individual to view the collection, which is valued highly.

d. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

e. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

f. Individuals whose sexual interest in children or images of children has led them to purchase access to paid websites or other commercial sources of child pornography frequently maintain the financial records of those transactions at their residences.

FACTS ESTABLIHING PROBABLE CAUSE

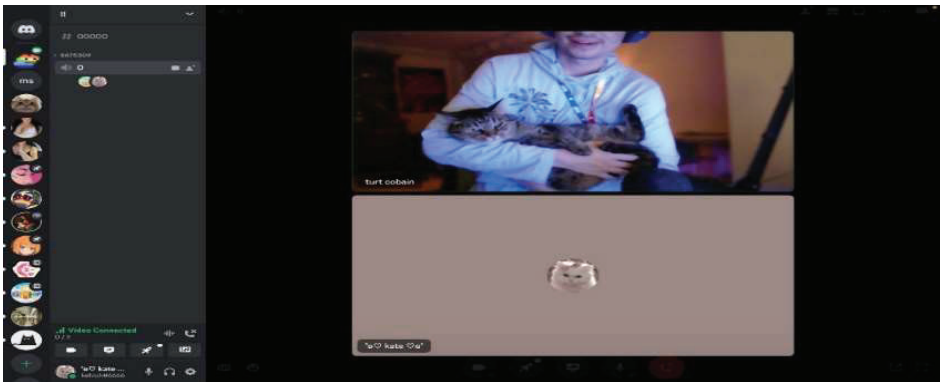
MV1

37. In September 2023, the FBI received information from the father of a minor female, date of birth (DOB) XX/XX/2009 (hereinafter MV1), concerning the possible online sexual exploitation of MV1 via Discord by an individual who self-identified as Michael David Seeds ("SUBJECT"), DOB 03/10/1998, residential address 43233 Lighthouse Pl., Chantilly, VA 20152. MV1 knew the SUBECT as "Mikey". Chantilly, VA is located within the Eastern District of Virginia.

38. In October 2023, MV1 underwent a Child and Adolescent Forensic Interview (CAFI) at the FBI Houston Field Office. MV1 disclosed that sometime on or around June 28, 2023,

she met the SUBJECT online in the public Discord server "egirlparadise."[1] The SUBECT shared with MV1 that he was 25 years old, and initially MV1 told the SUBJECT that she was 19 years old. Within approximately one week of communication, MV1 disclosed that she was actually 14 years old. The SUBJECT initially stated that he no longer wanted to communicate with MV1, as her being underage made him uncomfortable. However, within a few days, the SUBJECT reengaged with MV1 to update her on his missing cat and to inquire as to how she was doing. From this point, communication between MV1 and the SUBJECT resumed via DISCORD.

39. At the time, MV1 utilized a DISCORD account with the display name "kehioh", and the SUBJECT utilized a DISCORD account with the display name "turt cobain."[2] See below screenshot of a live DISCORD call with a man matching the physical description of the SUBJECT holding a cat, and the display name "turt cobain" in the bottom left corner of his photo box:



[1] A Discord server is the main chat forum on DISCORD, which can be thought of as micro-communities within Discord. While most servers are smaller private servers and require an invitation to join, some are larger public servers. Servers are used to ask/answer questions, share jokes or memes, and connect with others with similar interests. Servers allow users to chat via voice, video, or text.

[2] A display name is how you show up on DISCORD and how the user would like to be known to the community. Display names are not unique to each user. A username is a name unique to the user, serving as a unique identifier for each user. Usernames can be used to add friends and verify who you are talking to.

40. MV1 and SUBJECT continued to communicate on DISCORD in public servers to include "egirlparadise", "chillbar", and "chillzone", as well as via direct message and the call function[3] available on DISCORD.

41. Once contact between MV1 and SUBJECT had been reestablished, the SUBJECT purchased and created a new DISCORD account with the Nitro[4] subscription feature. The SUBJECT then gifted this account to MV1 and provided her with the display name "e_victim". The SUBJECT told MV1 that he called it "e_victim" because he often commented that he was a predator, but MV1 said she believed this to be a joke. MV1 understood that the SUBJECT created MV1 this account so that the original conversation when she claimed to be 19 and later disclosed her true age of 14 would be gone. The SUBJECT and MV1 communicated on this new account moving forward.

42. The SUBJECT frequently changed his DISCORD display name and made new accounts all together. During the CAFI of MV1, and via documents provided to investigators, MV1 shared the following list of DISCORD display names and/or usernames that were utilized by the SUBJECT:

stupidtrashpig
elobooster99
Variations of the "N" word plus the word "lover" plus several numbers
gangmemberryan
dylanshusband
Oh#0001
maddmikey4
God
michaelseeds

[3] A Direct Message is a message that is sent directly from the sender to the recipient and is not connected to a DISCORD server. Once in a direct message forum with a DISCORD user, a video call can occur by pressing the video call function in the menu bar.

[4] According to discord.com/nitro, Nitro is a subscription service within Discord that unlocks additional features within the platform such as custom emojis, the ability to upload bigger files, and profile customization.

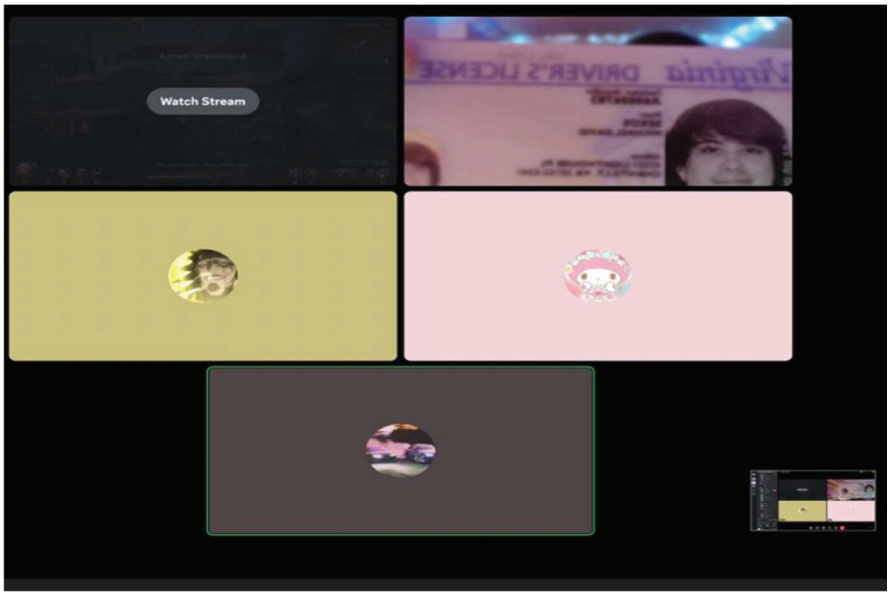
fishbones
F1SHB0N3S
KCJ
Oh
The Giggler
Mikey
Darth Kassadin
Unknown player
DEATH
L9 ROCKETEER
turt Cobain
cutie
XD

43. While the SUBJECT frequently created new account display names and usernames to communicate with MV1, MV1 knew that it was the same user because often times, their previous chats would still be present in the chat box.[5] Additionally, MV1 recognized the SUBJECT's voice during voice calls and face during video calls.

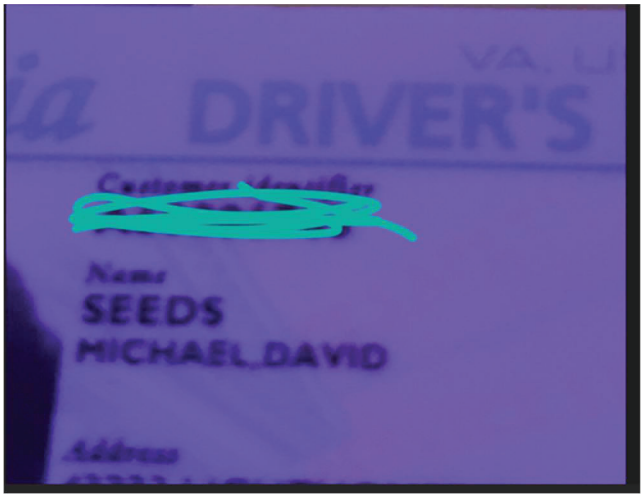
44. At one point, the SUBJECT shared with MV1 that his home address was 43233 Lighthouse Pl., South Riding, Virginia.[6] On a live call, the SUBJECT displayed his Virginia driver's license to MV1 and several others in a chat group. A screenshot of the license being held up to the camera was located during forensic imaging of MV1's laptop. See this image below:

[5] From my training and experience with DISCORD, when a user changes their display name, the chat histories associated to that account would remain. However, when a user creates a new username, it functions as a new account and would maintain its own chat history and friend list.

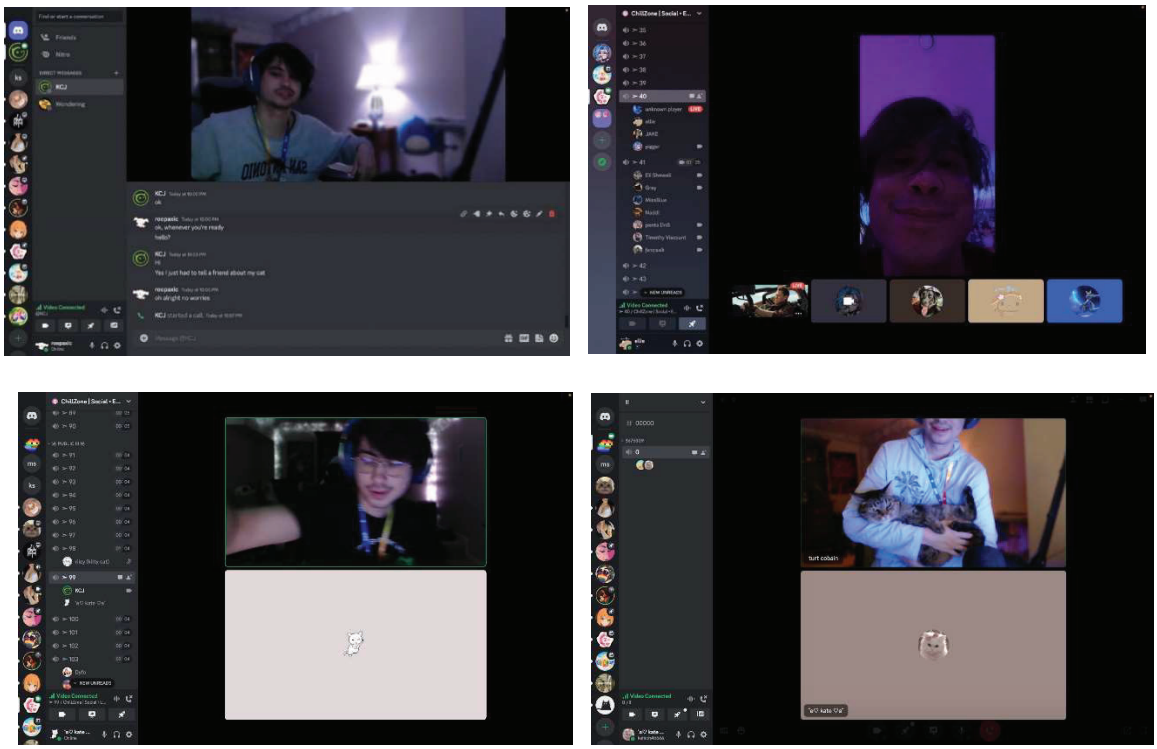
[6] Though the SUBJECT's driver's license photo indicated his stated his residence as Chantilly, South Riding is a census-designated place approximately 4 miles from Chantilly.



45. During additional imaging, a closer-up and clearer image of the SUBJECT's license was located, bearing name "Michael David Seeds". This license appears to be issued in the state of Virginia. See this image below:



46. MV1 captured screenshots of several live video calls with the SUBJECT via DISCORD, several of which show various views of the SUBJECT's face. See examples of these screenshots below:



47. During MV1's CAFI, MV1 was shown a copy of the driver's license photograph for the SUBJECT. MV1 positively identified the person in the photo as the SUBJECT, whom she referred to as "Mikey" and with whom MV1 had been participating in voice and video calls with via DISCORD.

48. In approximately August 2023 via DISCORD, the SUBJECT directed MV1 to produce sexually explicit images and videos of herself. MV1 complied with the SUBJECT's instruction to produce nude images of herself. The SUBJECT gave MV1 examples of how to pose in these images and later told MV1 that he would "cum" to her photos. During digital review of MV1's digital media, several nude images of a young female were located. The images are consistent with both the complexion of MV1 and the content MV1 described in her CAFI.

49. During DISCORD calls, MV1 recalled the SUBJECT telling her to "prop your camera up and go to town brother," requesting that she masturbate using her fingers. During the CAFI, MV1 disclosed that at the SUBJECT's request, she set up her camera and recorded and sent

the SUBJECT a video of herself masturbating. After this initial video, MV1 received several requests from the SUBJECT to record additional videos of herself masturbating, specifically asking her to crawl around naked on her bed, place her hands on her knees and stick her butt up, or to ride on and "cum" on her pillow. MV1 felt uncomfortable with these additional requests and declined to produce these additional videos.

50. During forensic review of MV1's laptop computer, the video mentioned by MV1 was not located, however an image was located that appears to be a screenshot of a video. The image is of a young female and shows her body from the area just above her breasts to her mid-thigh. The female's right leg is propped up on something and her right hand is over the top of her vagina. The female's ring finger and middle finger appear to be curved upwards, penetrating her vagina. The image appears to depict a young female masturbating.

51. During MV1's CAFI, she shared that the SUBJECT sent MV1 an image via Snapchat of his hands down his pants but did not expose his genitalia. During forensic review of MV1's laptop computer, a photo was located that depicted a hand placed under the front of a man's pants. The angle of the photo indicated the taker of the photo was also the subject of the photo.

52. During MV1's CAFI, MV1 disclosed that the SUBJECT instructed her that in front of his friends, she was to relay that she was 19 years old. The SUBJECT provided "rules" for MV1 to abide by when they were in live DISCORD servers where his friends were present. For example, the SUBJECT directed MV1 to introduce herself as her first name, when she typically introduced herself by her middle name. MV1 was also directed to claim a different location of residency when asked. Despite these "rules" to mislead friends, MV1 recalled an

occasion where she spoke with one of the SUBJECT's friends who stated that MV1 was "the fifth girl this month."

53. In addition to sexually focused conversation and remarks from the SUBJECT to MV1, the SUBJECT also would often utilize violent or aggressive language towards MV1. A screenshot of a conversation between the SUBJECT and MV1 was located on MV1's device, bearing one of the usernames and/or display names MV1 knew the SUBJECT to utilize, "XD". Relevant portions of this conversations are transcribed below:

SUBJECT: *im*

i wanna fuck

and then

cry

MV1: *why cry*

SUBJECT: *and beat the fuck out of u*

54. During MV1's CAFI, MV1 explained that the SUBJECT discussed gory things with her such as his desire to wear MV1's face as a mask, dismember her limbs, and kill her. Forensic imaging of MV1's devices identified a screenshot captured by MV1 of conversations with the SUBJECT using one of the usernames and/or display names MV1 knew the SUBJECT to utilize, "Darth Kassadin". This image is shown below:

55. During the CAFI, MV1 shared that on August 25, 2023, MV1 sent the SUBJECT via DISCORD a photo of several pills in her hand. The SUBJECT encouraged MV1 to commit suicide and told MV1 that he sold MV1's sexually explicit photographs and videos. To demonstrate he was still in possession of MV1's sexually explicit photos and videos, the SUBJECT then sent MV1 approximately five photos of MV1's exposed chest and a video of MV1 masturbating. The SUBJECT then encouraged MV1 to turn on her camera and prove that she would follow through with a suicide attempt. On a live call and at the encouragement of the SUBJECT, MV1 consumed the handful of pills, which were prescription medication. MV1 overdosed but survived. Later the same evening, MV1 shared with her parents what happened.

56. Throughout the course of various database queries conducted on the SUBJECT, law enforcement learned that the SUBJECT resides at 43233 Lighthouse Pl., Chantilly VA 20152. The full name that the SUBJECT provided to MV1 matches the SUBJECT's full legal name as it is revealed on his driver's license. The SUBJECT also displayed his full legal name via his driver's license during a live DISCORD call. While the address cannot be seen in its entirety on the image of his license captured by MV1, the house number does appear to be a five-digit number before the street name. A five-digit number appears to be in agreeance with the SUBJECT's known address as listed above.

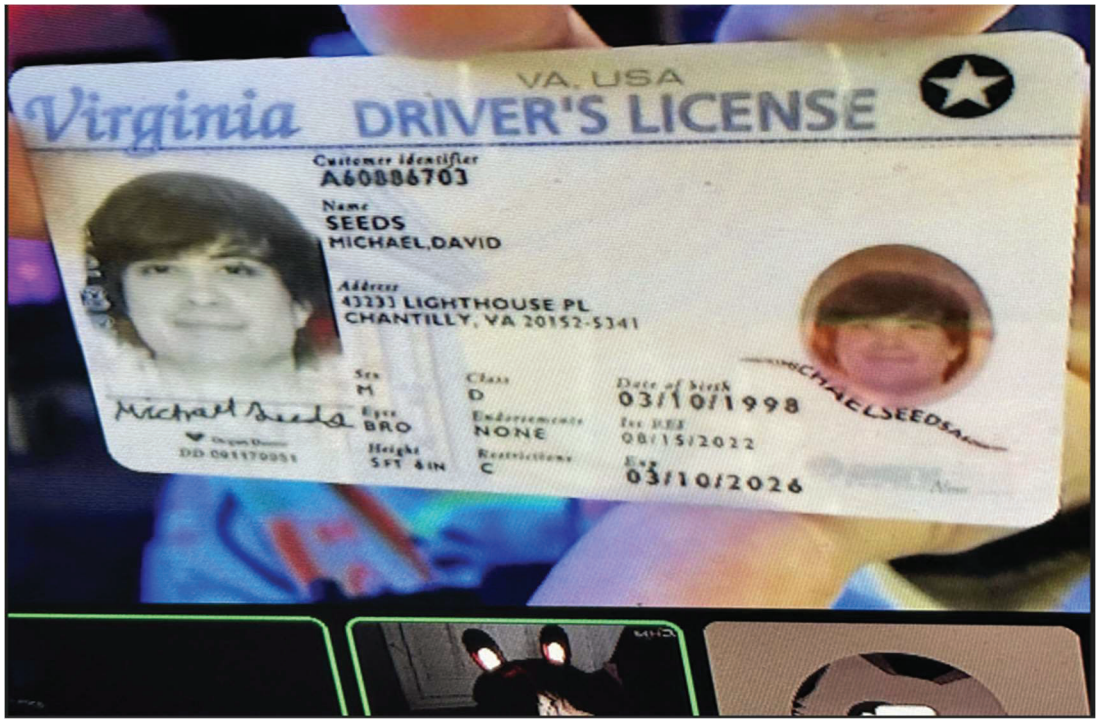
57. Lastly, the image displayed on SUBJECT's driver's license as shown in the DISCORD call is a direct match to the driver's license photo that law enforcement obtained from the Department of Motor Vehicles (DMV), as pictured below.

FBI Tip

58. In January 2024, the FBI received information from two adult complainants, C1 and C2, with no relation to MV1. The adult complainants provided information that they met the SUBJECT on DISCORD server "chillzone"[7] in December 2023 and began to correspond online. The SUBJECT then invited C1 and C2 to a private server with approximately 6 online users. After C1 and C2 were in the new private server, the SUBJECT invited a friend to the group who later reached out to C1 in a private chat, stating that the SUBJECT was being "creepy" towards her.

59. One on occasion while either in the larger public DISCORD server or in the smaller private server, the SUBJECT held his driver's license up to the camera. C1 and C2 learned that another group member had taken a screenshot of the SUBJECT holding up his driver's license. C1 and C2 retrieved that image prior to filing their complaint. See image of the driver's license below:

[7] "chillzone" was one of the servers through which MV1 and SUBJECT communicated, previously referenced in paragraph 40.



60. C1 reported that the SUBJECT began direct messaging her in ways she found uncomfortable, by "obsessively flirting" with her, despite knowing she was in a relationship with C2. The SUBJECT later learned that C1 and another user were talking about SUBJECT privately, so the SUBJECT began to harass and threaten C1 by threatening to rape, dox, or shoot her in the head. At that point, C1 and C2 submitted information to the FBI. C1 and C2 provided information that SUBJECT utilized Discord accounts with the following usernames and/or display names:

a. :3
b. kitty.face
c. hex.code.f

61. DISCORD requires users to have a username. Users pick a unique username and a display name, which need not be the same. Before May 2023, usernames were generated by a user then followed by a hashtag and assigned a unique four-digit discriminator (i.e. OneTwoThree#1234). Both username and display name are dynamic and may be changed by the

user after creation. Every DISCORD account is also assigned a user identification number ("UID") upon creation of the account, which is a static 18- or 19-digit number coded to the account. The UID cannot be changed. The UIDs of other users can be viewed by enabling "Developer Mode" within a DISCORD account.

62. Although MV1, C1, and C2 provided usernames and/or display names used by the SUBJECT, no DISCORD User IDs for the SUBJECT were then known or provided.

Identification of SUBJECT

63. In February 2024, legal process was served to DISCORD for subscriber information associated with username hex.code.f (request DISC-10468). DISCORD provided the following subscriber information:

User ID: 1142201852792934541
Username: hex.code.f#0
Email: gangmemberryan@proton.me[8]
Email verified: Yes
Phone number: Not found
Registration IP: Not found
Registration Time (UTC): 2023-08-18 21:02:22
Last Seen Time (UTC): 2023-12-23 12:21:18
Last Seen IP: 73.152.3.0

Additional legal process was served on DISCORD regarding subscriber information associated with User ID: 1142201852792934541, but DISCORD rejected this request noting that it had already produced data for the target account.

64. In March 2024, legal process was served to DISCORD for subscriber information for any DISCORD accounts associated with gangmemberryan@proton.me (request DISC-10677). DISCORD provided the following:

User ID: 1142201852792934541

[8] As noted in paragraph 42, "gangmemberryan" was among the SUBJECT's DISCORD usernames and/or display names provided by MV1.

Username: hex.code.f#0
Email: gangmemberryan@proton.me
Email verified: Yes
Phone number: Not found
Registration IP: Not found
Registration Time (UTC): 2023-08-18 21:02:22
Last Seen Time (UTC): 2023-12-23 12:21:18
Last Seen IP: 73.152.3.0

DISCORD also provided IP address history for the account between 2023-12-23 and 2023-08-18. Of the approximately 1,000 addresses provided, approximately 867 of the account history was at IP address 73.152.3.0.

65. In March 2024, legal process to Comcast confirmed that IP address 73.152.3.0 is hosted at 43233 Lighthouse Pl., Chantilly, VA 20152, the SUBJECT's residence.

In May 2024, a preservation request (DISC-14097) was issued to DISCORD regarding any/all accounts related to:

gangmemberryan
Dylanshusband
Oh#0001
stupidtrashpig
maddmikey4
god
elobooster99
KCJ
Oh
The Giggler
Gang Member Ryan
Mikey
Darth Kassadin
unknown player
DEATH
god
ELOBOOSTER69
L9 ROCKETEER
turt cobain
DOOMGUY
cutie
XD

DISCORD responded that they were unable to locate user accounts with identifiers: stupidtrashpig, Gang Member Ryan, Darth Kassadin, ELOBOOSTER69, turt cobain, or L9 ROCKETEER. Discord noted they were unable to confirm a user account with identifiers: gangmemberryan, Oh#0001, maddmikey4, god, KCJ, Oh, The Giggler, Mikey, unknown player, DEATH, god, DOOMGUY, cutie, or XD.

66. Based on DISCORD's response to preservation request DISC-14097, in May 2024, legal process was served to Discord for subscriber information associated with username elobooster99 (request DISC-14250). DISCORD provided the following information:

> User ID: 1142201852792934541
> Username: hex.code.f#0
> Email: gangmemberryan@proton.me
> Email verified: Yes
> Phone number: Not found
> Registration IP: Not found
> Registration Time (UTC): 2023-08-18 21:02:22
> Last Seen Time (UTC): 2023-12-23 12:21:18
> Last Seen IP: 73.152.3.0

67. As a result of all aforementioned legal process, this affiant has determined that DISCORD username "hex.code.f," which was provided by C1 and C2 in January 2024, is connected to UID 1142201852792934541 and the email address "gangmemberryan@protonmail.com." "Gangmemberryan" was one of the usernames for the SUBJECT that was provided by MV1 during her CAFI. The registration date for the UID 1142201852792934541 was 08/18/2023. This date is within the timeframe provided by MV1 during which she received requests from the SUBJECT to produce sexually explicit images and videos of herself. The registration date also precedes 08/25/2023, the date on which the SUBJECT encouraged MV1 to attempt suicide and sent MV1 the five photos of MV1's exposed chest and a video of MV1 masturbating, as referenced in paragraph 55.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

68. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular Title 18, United States Code, Sections 2703(a), (b)(1)(A), and (c)(1)(A), by using the warrant to require DISCORD to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. After disclosure, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

69. Based on the information set forth above, I submit there is probable cause to believe that Michael David Seeds is the owner of the SUBJECT ACCOUNT, as further identified in Attachment A, of which contains evidence, fruits, or instrumentalities and/or contraband related to the SUBJECT OFFENSES. I therefore request the Court issue the proposed search and seizure warrant in order to search the SUBJECT ACCOUNT for items described in Attachment B.

(Continued on next page)

70. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. Because the warrant will be served on DISCORD, who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

Olivia Temrowski
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to in accordance
with Fed. R. Crim. P. 4.1 by telephone
on August 16, 2024:

Digitally signed by Ivan Davis
Date: 2024.08.16 14:41:04 -04'00'

The Honorable Ivan D. Davis
United States Magistrate Judge
Alexandria, Virginia

ATTACHMENT A

Property to Be Searched

This warrant applies to information from at least May 1, 2023 until February 1, 2024 associated with the known DISCORD user Michael David Seeds, as well as information in the possession of DISCORD and associated with the following TARGET ACCOUNT:

- User identification number (UID) 1142201852792934541

This information is stored at premises owned, maintained, controlled, or operated by Discord Inc., an electronic communications service headquartered at 440 De Haro Street, Suite 200, San Francisco, CA 94107.

ATTACHMENT B

Things to be Seized and Procedures to Facilitate Execution of the Warrant

I. Information to be Disclosed by Discord, Inc. ("DISCORD") to Facilitate Execution of the Warrant

To the extent that the information described in Attachment A is within the possession, custody, or control of DISCORD, including any information that has been deleted but is still available to DISCORD, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), DISCORD is required to disclose the following information to the government for the TARGET ACCOUNT listed in Attachment A:

a. All contents of all wire and electronic communications associated with the TARGET ACCOUNT for the period May 1, 2023 through February 1, 2024, including:

i. All e-mails, communications, or messages of any kind associated with the TARGET ACCOUNT, including stored or preserved copies of messages sent to and from the TARGET ACCOUNT, deleted messages, and messages maintained in trash or any other folders or tags or labels, as well as all header information associated with each e-mail or message, and any related documents or attachments;

ii. All records or other information stored by subscriber(s) of the TARGET ACCOUNT, including address books, voice and voice-over-IP data, contact and buddy lists, calendar data, pictures, videos, notes, texts, links, user profiles, account settings, access logs, and files;

iii. All records pertaining to communications between DISCORD and any person regarding the TARGET ACCOUNT, including contacts with support services and records of actions taken;

iv. All stored passwords, including passwords stored in clear text and hash form, and for any hashed values that include a salt, DISCORD shall provide the salt value used to compute the stored password hash value, and any security questions and answers;

v. All search history and web history, including web clicks or "History Events," by the user of the TARGET ACCOUNT;

vi. All web browsing activities that are identifiable with the TARGET ACCOUNT; and

vii. Any and all logs of user activity and user agent string, including: web requests or HTTP requests; any logs containing information such as the Requestor's IP address, identity and user identification number ("UID"), date and timestamp, request URI or URL, HTTP protocol version, referrer, and other user agent string information; login tracker logs; account management logs; and any other information concerning other e-mail or social media accounts accessed or analytics related to the TARGET ACCOUNT.

b. All other records and information, including:

i. All subscriber information, including the date on which the TARGET ACCOUNT was created, the length of service, the IP address used to register the target account, the subscriber's full name(s), screen name(s), any alternate names, other account names or e-mail addresses associated with the target account, linked accounts, telephone numbers, physical addresses, and other identifying information regarding the subscriber, including any removed or changed names, email addresses, telephone numbers, or physical addresses, the types of service utilized,

account status, account settings, login IP addresses associated with session dates and times, as well as means and source of payment, including detailed billing records, **and including any changes made to any subscriber information** or services, including specifically changes made to secondary e-mail accounts, phone numbers, passwords, identity or address information, or types of services used, and including the dates on which such changes occurred, for the following accounts:

(1) The TARGET ACCOUNT;

(2) Any other account associated with the TARGET ACCOUNT, including by means of sharing a common secondary, recovery, or alternate **e-mail address listed in subscriber records** for the TARGET ACCOUNT or by means of sharing a **common phone number or SMS number listed in subscriber records** for the TARGET ACCOUNT; and

(3) Any other account accessed by a device with an identifier responsive to the device identifiers called for in Section I.b.iii, below.

ii. All user connection logs and transactional information of all activity relating to the TARGET ACCOUNT described above in Section I.a, including all log files, dates, times, durations, data transfer volumes, methods of connection, IP addresses, ports, routing information, dial-ups, and locations;

iii. Any information identifying the device or devices used to access the TARGET ACCOUNT, including any Android ID, Advertising ID, unique application number, hardware model, operating system version, unique device identifier, Global Unique Identifier or "GUID," serial number, mobile network

information, phone number, device serial number, MAC address, Electronic Serial Number ("ESN"), Mobile Electronic Identity Number ("MEIN"), Mobile Equipment Identifier ("MEID"), Mobile Identification Number ("MIN"), Subscriber Identity Module ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber Identifier ("IMSI"), International Mobile Equipment Identity ("IMEI"), or Apple advertiser ID or ID for advertisers ("IDEFA"), and any other information regarding the types of devices used to access the TARGET ACCOUNT or other device-specific information; and

iv. Any information showing the location of the user of the TARGET ACCOUNT, including while sending or receiving a message using the TARGET ACCOUNT or accessing or logged into the TARGET ACCOUNT.

Within **14 days** of the issuance of this Warrant, DISCORD shall deliver the information set forth above.

II. Information to be Seized by the Government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations 18 U.S.C. §§ 2251(a)(1), 2252(a)(2) and 2252(a)(4)(B), including the following:

a. Any messages pertaining to the production, receipt, distribution, possession, and attempt of such and access with intent to view of child pornography;

b. All posted images and videos pertaining to the production, receipt, distribution, possession, and attempt of such and access with intent to view of child pornography;

c. All posted text communications and public postings that further the production, receipt, distribution, possession, and attempt of such and access with intent to view of child pornography;

d. All access logs, administrative logs, user logs and posting history that will assist in locating users;

e. Evidence indicating how and when the SUBJECT ACCOUNT was created, accessed or used, to determine the chronological and geographical context of account access, use, and events relating to the crimes under investigation and to the SUBJECT ACCOUNT;

f. Evidence indicating the SUBJECT ACCOUNT users' state of mind as it relates to the crimes under investigation;

g. The identity of the person(s) who created or used the SUBJECT ACCOUNT, including records that help reveal the whereabouts of such person(s); and

h. The identity of the person(s) who communicated with the SUBJECT ACCOUNT about matters relating to the production, receipt, distribution, possession, and

attempt of such and access with intent to view of child pornography, including records that help reveal their whereabouts.

i. All files of child pornography and child erotica.